

## Amendments to the Claims

1. (currently amended) A ~~versatile customizable security and filtering software embedded upon embodied in a computer-readable medium, the software capable of being installed on a computer and be used by a remote user who obtains anonymity on a global telecommunications network or by a local user,~~ the software comprising:

(a) an administrative module that a user interacts with for creating user accounts and configuring those user accounts, ~~and for configuring automated services,~~

the administrative module for accepting user inputs for configuration settings for inbound communications, ~~and for outbound communications~~ or for inbound and outbound communications, ~~and having list maintenance functions including list editing,~~

~~said administrative module for configuring a range of access levels and being capable of creating user accounts that have unique user names and passwords for each user account including an administrator account that is self-configuring and that controls automated services and selects for each account hard filtering or soft filtering, regular accounts with administrative privileges other than the privilege to create additional accounts, view information on any other accounts or configure automated services and regular accounts without administrative privileges and in addition a fourth type of user account namely one anonymous guest user account to be used in a manual launch of the software by general users who have no system based user name or password,~~

~~the administrative module for storing as encrypted files on hardware memory the configurations of the range of access levels for the user accounts created and the configurations of the automated services——~~

(b) an application server including

a domain filtering engine either capable of using ~~from the encrypted files~~ a friendly outbound list and an unfriendly outbound list only one of which is active at any given time ~~and an outbound exception list, and~~ or capable of using a friendly inbound list and an unfriendly inbound list only one of which is active at any given time or capable of both using a friendly outbound list and an unfriendly outbound list only one of which is active at any given time and using a friendly inbound list and an unfriendly inbound list only one of which is active at any given time, and a domain inbound exception list, the friendly outbound list, the unfriendly outbound list, the friendly inbound list, the unfriendly inbound list, ~~the outbound exception list and the domain inbound exception list~~ being uniquely configured for each user account,

the using of the friendly or unfriendly outbound lists by the domain filtering engine involving checking user requested web resources against the friendly or unfriendly outbound lists, the using of the friendly or unfriendly inbound lists by the domain filtering engine involving ~~capable of registering the request in a logfile of all web sites requested by a user and capable of performing domain filtering, said domain filtering including for inbound requests checking the identity of a requesting remote client against the friendly inbound or unfriendly inbound lists and domain inbound exception list maintained in the encrypted files and including for outbound requests checking local user and remote user requested domains, URLs and links against the friendly outbound list, unfriendly outbound list and outbound exception list and then with respect to both inbound and outbound requests for hard filtering unless overruled by the outbound exception list or domain inbound exception list either approving the request, terminating the request or terminating and re-routing the request without the knowledge of the user, and for soft filtering unless overruled by the outbound exception list or domain inbound exception list passing disapproved requests and sending an e-mail alert to authorized recipients~~

~~regarding the disapproved request, wherein, for requests that are terminated and re-rerouted, inbound communications are arranged so that an actual location of a highly sensitive resource is located in an unpublished location that is a replacement location to which requests rejected by the application server are rerouted, wherein clients of approved users are listed in the application server in the unfriendly inbound list and are sent by the application server to the replacement location, and wherein clients of unapproved users are not listed in the unfriendly inbound list and have their request sent to a published address that contains harmless information.~~

~~the application server acting internally to communicate with the domain filtering engine and acting externally as a proxy server that receives requests from HTTP clients, forwards the requests to servers, receives a server response and forwards the server response to the HTTP clients.~~

2. (original) The software of claim 1, wherein the domain filtering engine also has an optional alert system for hard filtering, for soft filtering or for both hard and soft filtering.

3. (previously presented) The software of claim 1, wherein the domain filtering engine has an outbound privacy shield for blocking disapproved character strings representing confidential information.

4. (canceled)

5. (canceled)

6. (currently amended) The software of claim 1, including an automated scheduler that controls a launching of the software ~~application-server~~ automatically and decides which user account to activate and when to shut off an access to a world wide web, and includes an automated list updater that updates the friendly inbound list, the unfriendly inbound list, the friendly outbound list and the unfriendly outbound lists for each user account from links on the web.

7. (canceled)

8. (canceled)

9. (currently amended) The software of claim 1, wherein the administrative module includes an editor, the editor including an editing pane, said editor also including an encryption function that generates one or more secret symmetric encryption keys, the one or more encryption keys being uniquely associated with a text ~~inputted~~ presented by a user ~~of in~~ the editing pane, said encryption function capable of encrypting ~~at the user's option~~ all or only a portion of an e-mail message selected by the user.

10. (currently amended) The software of claim 1, wherein the domain filtering further includes an ~~the~~ application server acting internally to communicate with the domain filtering engine and acting externally as a proxy server that receives requests from HTTP clients, forwards the requests to servers, receives a server response and forwards the server response to

the HTTP clients.

11. (original) The software of claim 1, wherein the administrative module is also capable of configuring an automated configuration script file for accessing the global telecommunications network.

12. (original) The software of claim 1, wherein for e-mail filtering includes an option of hard e-mail filtering in which an incoming e-mail is deleted from a user e-mail inbox and includes an option for soft filtering in which an incoming e-mail remains in the user e-mail inbox but is inaccessible to the user.

13. (currently amended) The software of claim 1, further including A versatile  
~~customizable security and filtering software embedded upon a computer-readable medium, the~~  
~~software comprising:~~

~~(a) an administrative module that a user interacts with for creating user accounts and configuring those user accounts, and for configuring automated services,~~

~~the administrative module for accepting user inputs for configuration settings for inbound communications and for outbound communications, and having list maintenance functions including list editing, list deleting, searching of lists, saving of lists, proxy chaining routing, adding and deleting users, interchanging lists and importing and exporting lists, \_\_\_\_\_~~

~~said administrative module for configuring a range of access levels and being capable of creating three types of user accounts that have unique user names and passwords for each user account including an administrator account that is self-configuring and that controls automated services and selects for each account hard filtering or soft filtering, regular accounts with administrative privileges other than the privilege to create additional accounts, view information on any other accounts or configure automated services and regular accounts without administrative privileges and in addition a fourth type of user account namely one anonymous guest user account to be used in a manual launch of the software by general users who have no system based user name or password,~~

~~the administrative module for storing as encrypted files on hardware memory the configurations of the range of access levels for the user accounts created and the configurations of the automated services \_\_\_\_\_~~

~~(b) an application server including~~

~~(i) a domain filtering engine capable of using from the encrypted files a friendly outbound list and an unfriendly outbound list only one of which is active at any~~

given time and an outbound exception list, and using a friendly inbound list and an unfriendly inbound list only one of which is active at any given time, and a domain inbound exception list, the friendly outbound list, the unfriendly outbound list, the outbound exception list, the domain inbound exception list, a friendly e-mail list and an unfriendly e-mail list being uniquely configured for each user account,

the domain filtering engine capable of registering the request in a logfile of all web sites requested by a user and capable of performing domain filtering, said domain filtering including domain inbound exception list maintained in the encrypted files and including for outbound requests checking local user and remote user requested domains, URLs and links against the friendly outbound list, unfriendly outbound list and outbound exception list and then with respect to outbound requests for hard filtering unless overruled by the outbound exception list or domain inbound exception list either approving the request, terminating the request or terminating and re-routing the request without the knowledge of the user, and for soft filtering unless overruled by the outbound exception list or domain inbound exception list passing disapproved requests and sending an e-mail alert to authorized recipients regarding the disapproved request, wherein, for requests that are terminated and re-rerouted, inbound communications are arranged so that an actual location of a highly sensitive resource is located in an unpublished location that is a replacement location to which requests rejected by the application server are rerouted, wherein clients of approved users are listed in the application server in the unfriendly inbound list and are sent by the application server to the replacement location, and wherein clients of unapproved users are not listed in the unfriendly inbound list and have their request sent to a published address that contains harmless information, and

(ii) a content filtering engine capable of performing content filtering including checking a content of a requested document against a friendly content inbound list, an unfriendly content inbound list, and ~~a content exception list taken from the encrypted files, the friendly content inbound list, the unfriendly content inbound list,~~ only one of the friendly content inbound list and the unfriendly content inbound list being active at any given time, the friendly content inbound list and the unfriendly content inbound list being uniquely configured for each user account, and ~~the content exception list being uniquely configured by each user,~~ and if the content filtering involves then for hard filtering then against the unfriendly content inbound list either passing the requested document if the said content of the requested document is not on the unfriendly content inbound list or ~~unless overruled by the content exception list~~ rejecting the requested document if the said content of the requested document is on the unfriendly content inbound list and for hard filtering against the friendly content inbound list either ~~unless overruled by the content exception list~~ passing the requested document if the said content of the requested document is on the friendly content inbound list or rejecting the requested document if the said content of the requested document is not on the friendly content inbound list and if the content involves for soft filtering then against the unfriendly content inbound list either approving the content of the requested document and passing the requested document if the said content is not on the unfriendly content inbound list or ~~unless overruled by the content exception list~~ rejecting the content of the requested document and passing a remainder of the requested document if the said content is on the unfriendly content inbound list and ~~for soft filtering~~ against the friendly content inbound list either ~~unless overruled by the content exception list~~ passing rejecting



the requested document if parts of the content is not on the friendly content inbound list or passing the requested document and ~~highlighting the content of the requested document if the said content is on the friendly content inbound list, said content filtering also including e-mail filtering that checks a subject, a sender's address and a sender's domain against an unfriendly e-mail list, a friendly e-mail list and an e-mail exception list,~~—

~~the application server acting internally to communicate with the domain filtering engine and with the content filtering engine and acting externally as a proxy server that receives requests from HTTP clients, forwards the requests to servers, receives a server response and forwards the server response to the HTTP clients.~~

14. (currently amended) A ~~versatile customizable security and filtering software embedded upon~~ embodied in a computer-readable medium, the software, comprising:

(a) an administrative module that a user interacts with for creating user accounts and configuring those user accounts, and ~~for configuring automated services,~~

the administrative module for accepting user inputs for configuration settings for inbound communications, outbound communications or inbound and outbound communications and having list maintenance functions including list editing, list deleting, searching of lists, saving of lists, proxy chaining routing, adding and deleting users, interchanging lists and importing and exporting lists, —————

————— said administrative module for configuring a range of access levels and being capable of creating three types of user accounts that have unique user names and passwords for each user account including an administrator account that is self-

~~configuring and that controls automated services and selects for each account hard filtering or soft filtering, regular accounts with administrative privileges other than the privilege to create additional accounts, view information on any other accounts or configure automated services and regular accounts without administrative privileges and in addition a fourth type of user account namely one anonymous guest user account to be used in a manual launch of the software by general users who have no system-based user name or password,~~

~~the administrative module for storing as encrypted files on hardware memory the configurations of the range of access levels for the user accounts created and the configurations of the automated services~~

(b) ~~an application server including a content filtering engine capable of performing content filtering including checking a content of a requested document against a friendly content inbound list, and an unfriendly content inbound list, and a content exception list taken from the encrypted files, the friendly content inbound list, only one of the friendly content inbound list and the unfriendly content inbound list being active at any given time, the friendly content inbound list and the unfriendly content inbound list being uniquely configured for each user account, the unfriendly content inbound list and the content exception list being uniquely configured by each user, and if the content filtering involves then for hard filtering then against the unfriendly content inbound list either passing the requested document if the said content of the requested document is not on the unfriendly content inbound list or unless overruled by the content exception list rejecting the requested document if the said content of the requested document is on the unfriendly content inbound list and for hard filtering against the~~

friendly content inbound list either ~~unless overruled by the content exception list~~ passing the requested document if the said content of the requested document is on the friendly content inbound list or rejecting the requested document if the said content of the requested document is not on the friendly content inbound list and if the content filtering involves ~~for~~ soft filtering then against the unfriendly content inbound list either approving the content of the requested document and passing the requested document if the said content is not on the unfriendly content inbound list or ~~unless overruled by the content exception list~~ rejecting the content of the requested document and passing a remainder of the requested document if the said content is on the unfriendly content inbound list and ~~for soft filtering~~ against the friendly content inbound list either ~~unless overruled by the content exception list~~ passing rejecting the requested document if the said content is not on the friendly content inbound list or passing the requested document and ~~highlighting the content of the requested document~~ if the said content is on the friendly content inbound list, ~~said content filtering also including e-mail filtering that checks a subject, a sender's address and a sender's domain against an unfriendly e-mail list, a friendly e-mail list and an e-mail exception list, ———~~

~~the application server acting internally to communicate with the domain filtering engine and with the content filtering engine and acting externally as a proxy server that receives requests from HTTP clients, forwards the requests to servers, receives a server response and forwards the server response to the HTTP clients.~~

15. (canceled)

16. (canceled)

17. (previously presented) The software of claim 14, wherein the content filtering engine has an inbound privacy shield for blocking scripting language functions for particular user accounts.

18. (previously presented) The software of claim 13, wherein the content filtering engine, when performing hard filtering, can also replace a requested document that has been rejected with a replacement document selected by a user of the administrator account.

19. (new) The software of claim 1, wherein the domain filtering also includes with respect to both inbound and outbound requests for hard filtering either approving the request, terminating the request or terminating and re-routing the request

20. (new) The software of claim 1, wherein the domain filtering also includes with respect to both inbound and outbound requests for soft filtering passing disapproved requests and sending an alert to authorized recipients regarding the disapproved request.

21. (new) The software of claim 19, wherein the domain filtering also provides that, for requests that are terminated and re-rerouted, inbound communications are arranged so that an actual location of a highly sensitive resource is located in an unpublished location that is a replacement location to which requests rejected by the

software are rerouted, wherein clients of approved users are listed in the application server in the unfriendly inbound list and are sent by the application server to the replacement location, and wherein clients of unapproved users are not listed in the unfriendly inbound list and have their request sent to a published address that contains harmless information.

22. (new) The software of claim 10, wherein the application server, instead of acting externally as a proxy server, acts externally within a deployment of a chain of proxy servers including at least a first proxy server that receives requests from HTTP clients and forwards the requests through a zero or more intermediary proxy servers to a last proxy server, said last proxy server forwarding the requests to servers, and wherein the last proxy server receives a server response and forwards the server response through the zero or more intermediary proxy servers back to the first proxy server, which first proxy server forwards the server response to HTTP clients.

23. (new) The software of claim 1, wherein the domain filtering engine is capable of using from the administrative module a domain outbound exception list, is capable of using from the administrative module a domain inbound exception list and is capable of using from the administrative module a domain outbound exception list and a domain inbound exception list, the domain outbound exception list and the domain inbound exception list being uniquely configured for each user account.

24. (new) The software of claim 1, wherein the domain filtering, for soft filtering

involves passing disapproved requests and sending an e-mail alert to authorized recipients regarding the disapproved request.

25. (new) The software of claim 1, said administrative module having list maintenance functions including list editing, list deleting, searching of lists, saving of lists, adding and deleting users, and having list maintenance functions including list editing, interchanging lists and importing and exporting lists.

26. (new) The software of claim 25, said administrative module having proxy chaining functions including proxy chaining routing.

27. (new) The software of claim 1, said administrative module able to configure a range of access levels and being capable of creating three types of user accounts that have unique authentication credentials for each user account including an administrator account that is self-configuring and that controls automated services and selects for each account hard filtering or soft filtering, regular accounts with administrative privileges other than the privilege to create additional accounts, view information on any other accounts or configure automated services and regular accounts without administrative privileges.

28. (new) The software of claim 1, said administrative module able to create a fourth type of user account namely one anonymous guest user account to be used by general users who have no authentication credentials.

29. (new) The software of claim 1, wherein the administrative module is capable of creating, modifying or reading the configuration settings or is capable of storing the configurations settings in memory, cache, encrypted files, plain text files, storage devices, computer storage media or as web resources.

30. (new) The software of claim 1, wherein the administrative module is capable of configuring the range of access levels for the user accounts created and is capable of configuring automated services.

31. (new) The software of claim 1, wherein the administrative module is capable of configuring automated services.

32. (new) The software of claim 1, wherein the domain filtering engine is capable of performing domain filtering, said domain filtering including checking the identity of a requesting client against the friendly inbound or unfriendly inbound list and domain inbound exception list and including for outbound web-based resource requests either

- (i) checking user requested applications or
- (ii) checking user requested domains or
- (iii) checking user requested URLs or
- (iv) checking user requested addresses or
- (v) checking user requested links

against the friendly outbound list and/or the unfriendly outbound list and outbound exception list and then with respect to both inbound and outbound client communication requests for hard filtering unless overruled by the outbound exception list or domain inbound exception list either approving the request, terminating the request or terminating and re-routing the request.

33. (new) The software of claim 32, the soft domain filtering engine capable of performing domain filtering and for soft domain filtering unless overruled by the outbound exception list or domain inbound exception list passing disapproved requests and sending an alert to authorized recipients regarding the disapproved request.

34. (new) The software of claim 33, wherein the soft domain filtering engine, for soft filtering, passes disapproved requests and sends alerts to authorized recipients regarding the disapproved requests.

35. (new) The software of claim 1, wherein the software is programmed to check an identity of a user who logs in and who presents a unique authentication credential prior to checking an identity of a requesting client or requested resource.

36. (new) The software of claim 35, wherein the software is also programmed, upon a successful authentication of the user's credential, to use a configuration of the user's account to check the identity of the requesting client or requested resource.



37. (new) The software of claim 35, wherein the software is also programmed that if the software fails to authenticate the user, the first proxy server offers that user an opportunity to log in as an anonymous guest user.

38. The software of claim 1, wherein the computer-readable medium is in a computer.

39. The software of claim 1, wherein the computer-readable medium is in hardware.

40. (new) The software of claim 13, wherein for e-mail filtering includes an option of hard e-mail filtering in which an incoming e-mail is deleted from a user e-mail inbox.

41. (new) The software of claim 13, wherein for e-mail filtering includes an option of soft filtering in which an incoming e-mail remains in the user e-mail inbox but is inaccessible to the user.

42. (new) The software of claim 13, wherein the content filtering engine is capable of using from the administrative module an unfriendly hard content exception list and/or a friendly hard content exception list, and/or an unfriendly soft content exception list and/or a friendly soft content exception list, the unfriendly soft content exception list

and a friendly soft content exception list and unfriendly hard content exception list and the friendly hard content exception list, being uniquely configured for each user account.

43. (new) The software of claim 42, wherein the content filtering engine is capable for hard filtering against a friendly hard content inbound list, an unfriendly hard content inbound list, a friendly hard content exception list and an unfriendly hard content exception list, the friendly content inbound list, the unfriendly content inbound list, only one of the friendly content inbound list and the unfriendly content inbound list being active at any given time, and then for hard filtering against the unfriendly content inbound list either passing the requested document if the said content of the requested document is not on the unfriendly content inbound list or unless overruled by the unfriendly hard content exception list rejecting the requested document if the said content of the requested document is on the unfriendly content inbound list and for hard filtering against the friendly content inbound list either unless overruled by the friendly hard content exception list passing the requested document if the said content of the requested document is on the friendly content inbound list or rejecting the requested document if the said content of the requested document is not on the friendly content inbound list.

44. (new) The software of claim 42, wherein the content filtering engine is capable for soft filtering against the unfriendly content inbound list either unless overruled by the unfriendly soft content exception list approving the content of the requested document and passing the requested document if the said content is not on the unfriendly content inbound list or unless overruled by the unfriendly soft content

exception list rejecting the content of the requested document and passing a remainder of the requested document if the said content is on the unfriendly content inbound list and/or for soft filtering against the friendly content inbound list either unless overruled by the friendly soft content exception list rejecting the requested document if the said content is not on the friendly content inbound list or unless overruled by the friendly soft content exception list passing the requested document if the said content is on the friendly content inbound list.

45. (new) The software of claim 13, wherein a content filtering engine capable of using from the administrative module a soft content exception list, and using a hard content exception list, soft content exception list, and hard content exception list are being uniquely configured for each user account.

46. (new) The software of claim 13, wherein the content filtering engine, when performing soft filtering, can also replace a requested document that has been rejected with a replacement document selected by a user of the administrator account.

47. (new) The software of claim 14, said content filtering also including e-mail filtering that checks a subject, a sender's address and a sender's domain against an unfriendly e-mail list, and friendly e-mail list.

48. (new) The software of claim 14, wherein the content filtering engine is capable of using from the administrative module an email exception list, the e-mail

exception list being uniquely configured for each user account.

49. (new) The software of claim 48, said content filtering also including e-mail filtering that checks a subject, a sender's address and a sender's domain against an unfriendly e-mail list, a friendly e-mail list and an e-mail exception list.

50. (new) The software of claim 14, wherein the software is programmed to check an identity of a user who logs in and who presents a unique authentication credential prior to checking an identity of a requesting client or requested resource.

51. (new) The software of claim 50, wherein the software is also programmed, upon a successful authentication of the user's credential, to use a configuration of the user's account to check the identity of the requesting client or requested resource.

52. (new) The software of claim 50, wherein the software is also programmed that if the software fails to authenticate the user, the first proxy server offers that user an opportunity to log in as an anonymous guest user.

53. (new) The software of claim 14, wherein the computer-readable medium is in a computer.

54. (new) The software of claim 14, wherein the computer-readable medium is in hardware.